AppSentinels.ai
Application Security Re-invented

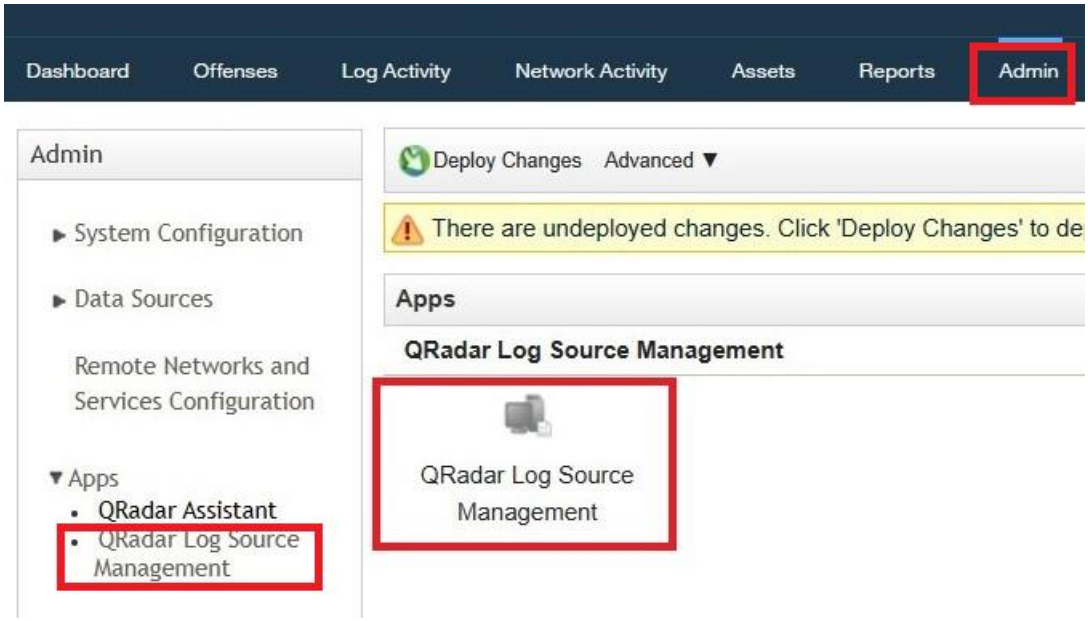
# QRADAR INTEGRATION

AppSentinels API Security Platform supports QRadar integration for the Security Events/Vulnerability Events using public APIs and using QRadar Universal CloudRest API.

The following steps has to be followed to configure the QRadar to fetch the events in regular interval.

# 1 Select Log Source Management

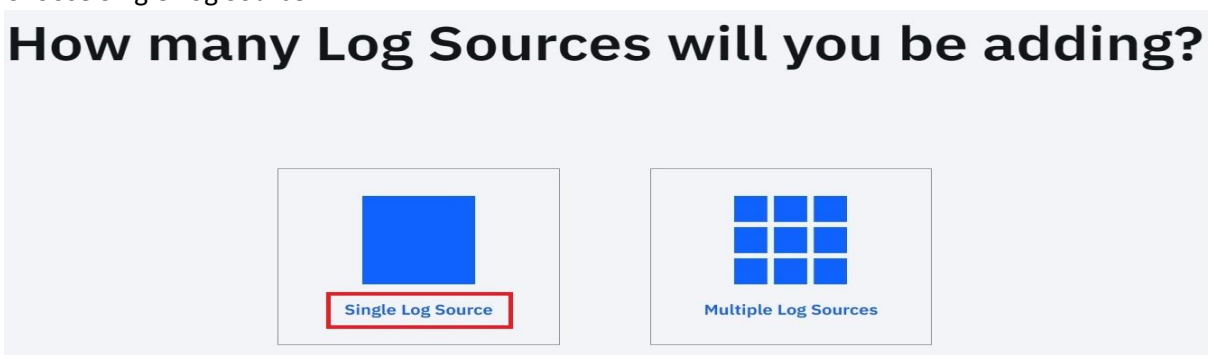
- Go to Admin -> QRadar Log Source Management
- Open the QRadar Log Source Management




# 2 Configuration New Log Source

Configure “New Log Source” to add AppSentinels events source.


Choose Single Log Source

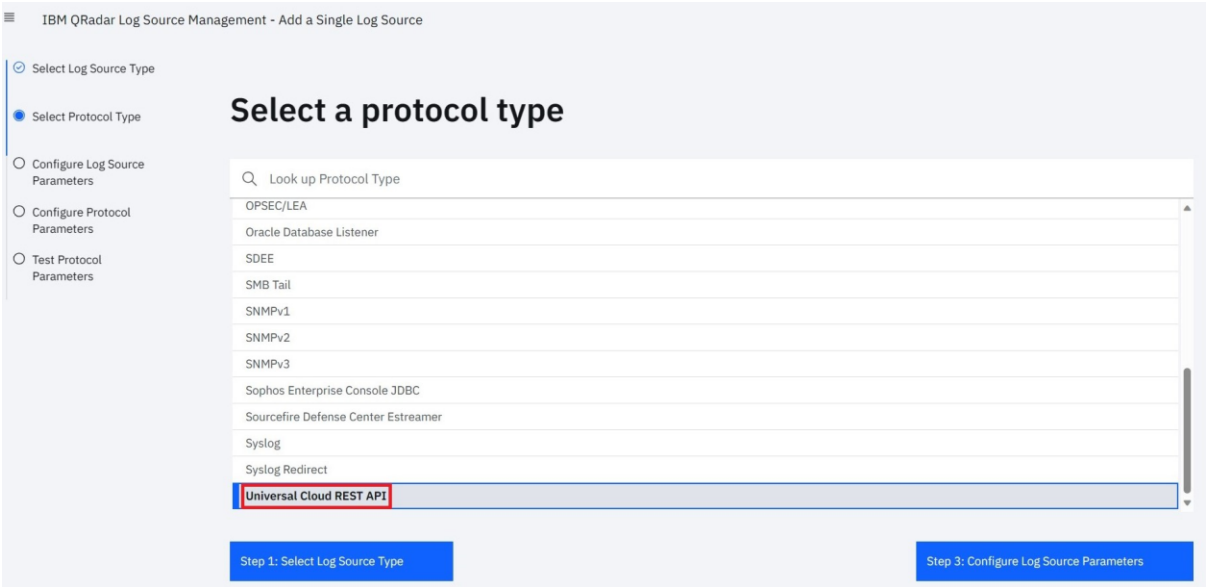


# 3 Select Log Source TYPE

Select “Universal DSM” as the Log Source Type

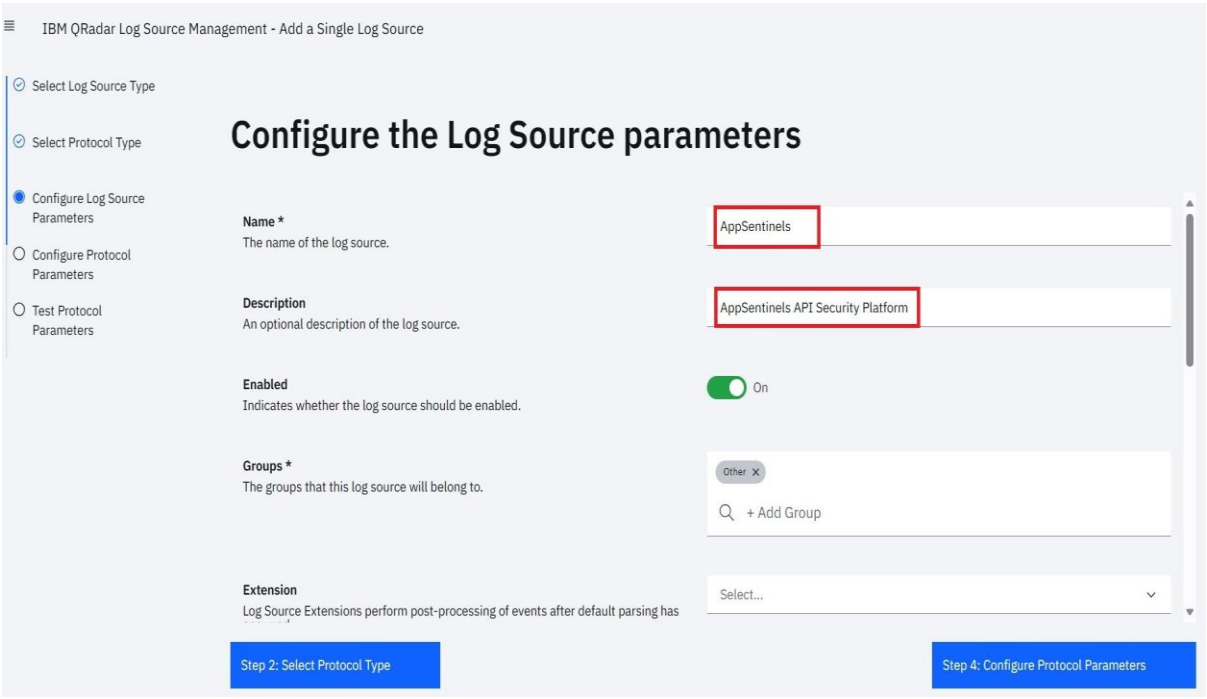

# 4 Select Protocol Type

Select “Universal Cloud REST API” as protocol type

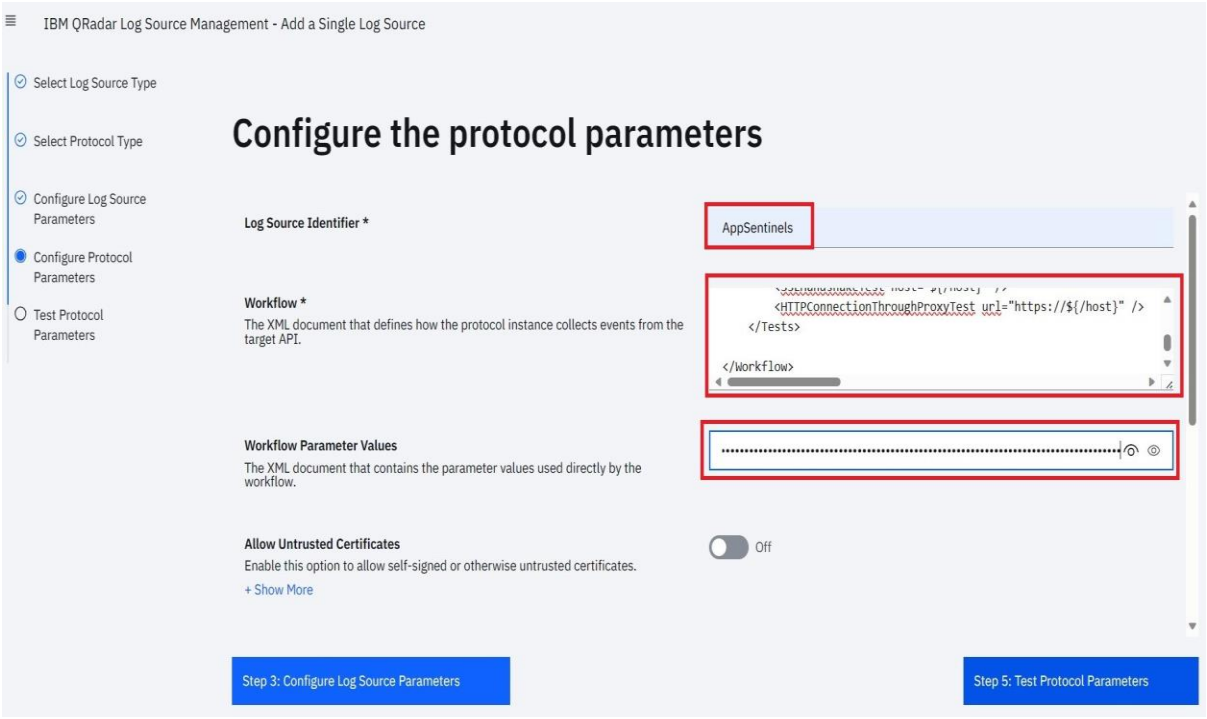


# 5 Configure Log Source Parameter

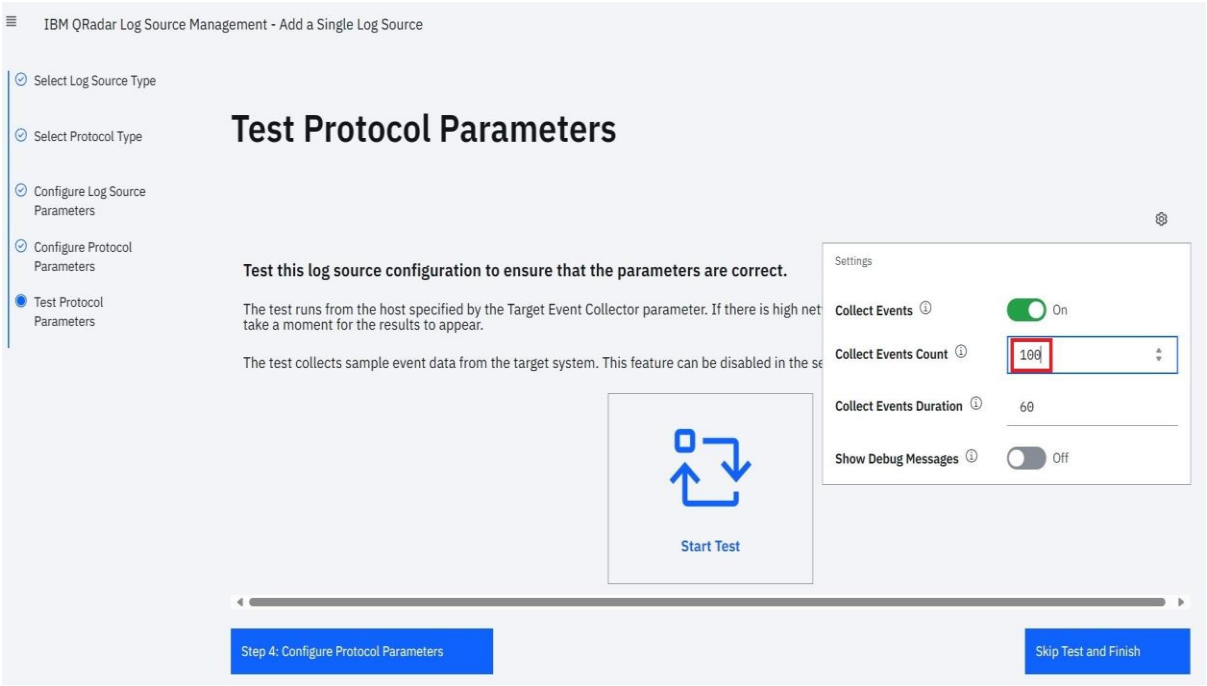
## 5.1 Configure the Log Source Parameters



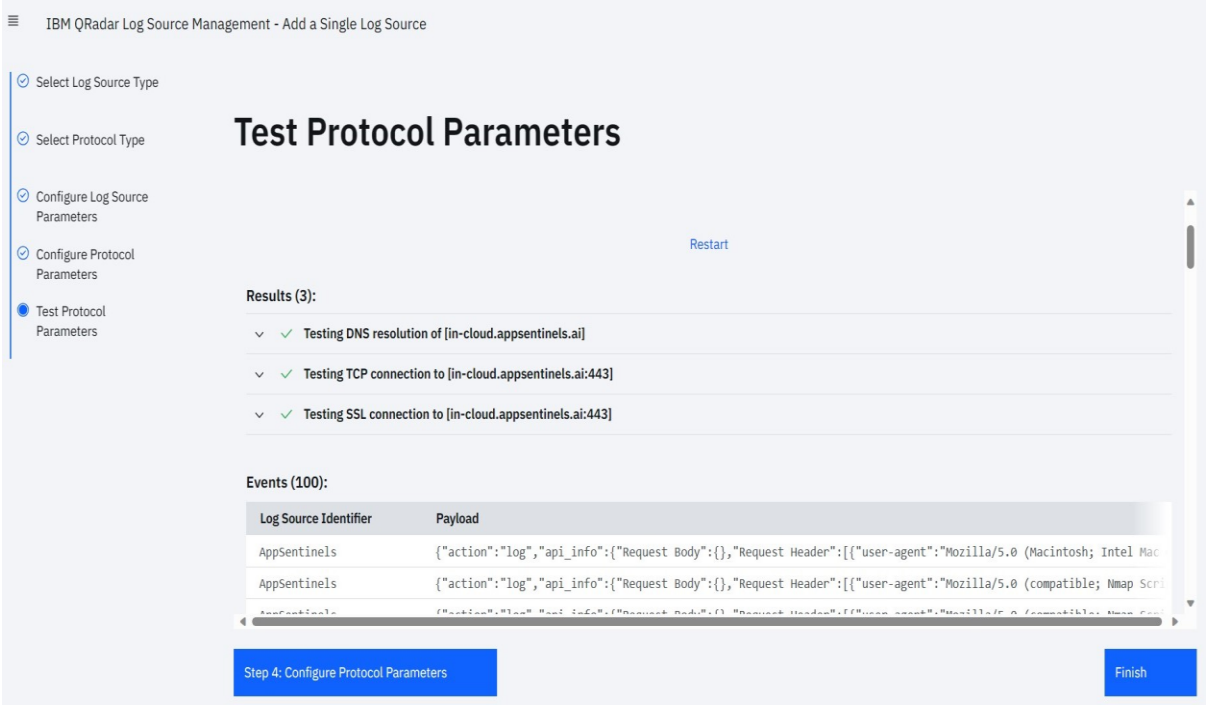

5.2 Update the workflow and workflow parameters. Refer the section Workflow Details section for details.



5.3 Configure the Protocol Parameters “Collect Events Count” as 100 (AppSentinels Platform provides maximum 100 events in response) and “Collect Events Duration” with the interval in secs to fetch the Security Events

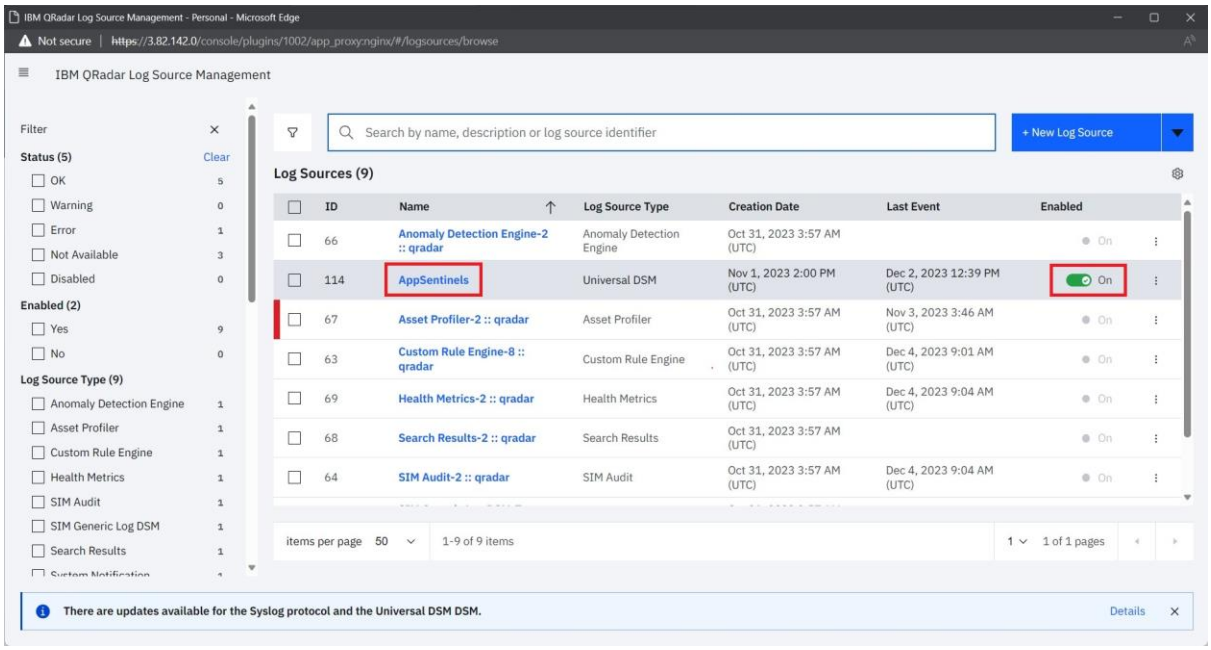



5.4 Test the configuration to confirm the events are retrieved by QRadar



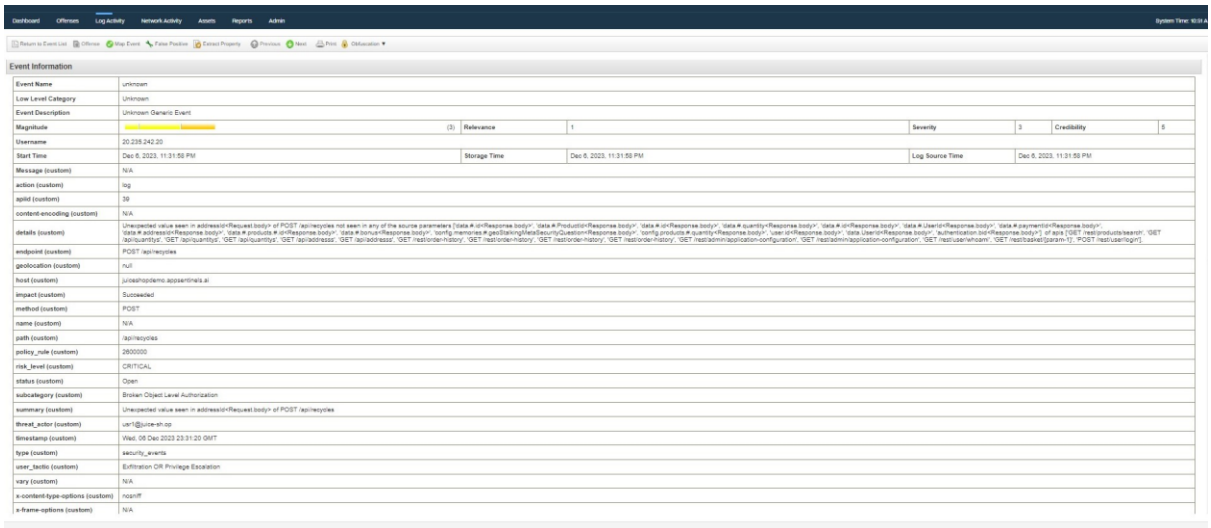
# 6 Confirm Log Source is added

AppSentinels should be listed in the Log Sources list and should be enabled.




# 7 Verify Events in JIRA

Generate Security events and verify the Security Events are retrieved by QRadar.



# 8 Mapping of Events field

AppSentinels Security Events fields uses API Security related parameters in the event details. Use the DSM Editor to map the AppSentinels Event parameters with standard fields of QRadar.

# 9 Workflow Parameters Details

AppSentinels has defined the workflow.xml and workflow.parameters.values.xml required for integrating AppSentinels API Security Platform events to QRadar.

The files can be downloaded from [https://storage.googleapis.com/appsentinels-deployment/index.html](https://storage.googleapis.com/appsentinels-deployment/index.html)

## 9.1 AppSentinels_workflow.xml

The severity of the events to be fetched should be updated in the appsentinels_workflow.xml file. The supported severity values are critical, major, minor and info.


## 9.2 AppSentinels_workflow.parameter.values.xml

```
<?xml version="1.0" ?>

<WorkflowParameterValues
xmlns="http://qradar.ibm.com/UniversalCloudRESTAPI/WorkflowParameterValues/V2">

   <Value name="host" value="in-cloud.appsentinels.ai"/>

   <Value name="apiKey" value="APIKEY"/>

   <Value name="orgName" value="ORGNAME"/>

   <Value name="appName" value="ORGNAME_APPNAME"/>

   <Value name="include_runtime_scan" value="false"/>

   <Value name="aggregation" value="true"/>

   <Value name="type" value="security_events"/>

</WorkflowParameterValues>
```

***apiKey*:** API KEY generated in the AppSentinels Platform for accessing the public APIs

***orgName*:** Organization Name as defined in the AppSentinels Platform

***appName*:** Application Name as defined in the AppSentinels Platform

***include_runtime_scan*:** To include the vulnerability events from the run time scan category. This configuration is applicable to vulnerability events.

***aggregation*:** To fetch only the parent attack or fetch all the attacks when the similar events are aggregated.

***type*:** Type of the event, could be security_events or vulnerabilities